LiNKDOOD ANTI-VIRUS

Linkdood Antivirus

Who is the target user?

Able to control from one cloud storage management all your endpoint, and want to update those virus databases immediately without the control of the third party.

BEYOND SECURITY LINKDOOD

Table of Content

Introduction

LINKDOOD Antivirus V3 is the private cloud virus prevention solution for enterprise users. With world-leading private cloud security system, users can customize cloud knowledge, which has the advantage of cloud virus killing and can prevent data leakage.

Based on various years' experience of endpoint security management, LINKDOOD Antivirus V3 is able to meet enterprise user's need of uniformly managing antivirus through multi-level control platform.

With light client as research direction, LINKDOOD Antivirus intends to reduce endpoint resource consumption. It can real-time protect endpoint and dynamically detect threats, which effectively prevent virus, unknown threats and APT attack.

Design Concept

LINKDOOD Antivirus follows the concept of process closed loop, which has detection mechanism in every link to ensure suspicious files not to be missed due to some link.

Boundary Protection Monitor file from the very beginning. Real-time monitoring of sensitive boundary interface such as visit website, download software and copy file, which precisely intercept dangerous file and prevent risk from entering your computer.

Real-time Monitoring Monitor all process. Once virus is found, it will automatically remove virus file or lock it from running.

Active Defense Through behavior analysis and multi-engine, it can actively detect potential threats, smartly mark risk level and block them.

Scheduled Scan Scan endpoint through Console Platform's operation so as to avoid virus infection due to user's randomness.

Cloud Identification Technology Through various mainstream antivirus engines, cloud VDC identify gray sample that client can't recognize.

Through above measures, the failure probability of virus detection is less than 0.1%. If unidentified gray sample found, we will manually analyze whether it is threat or not.

Figure 1

Market Analysis

Since 21st century, various network threat and hacker attack explosively increase with the feature of professionalized attack tools, commercialized purpose and organized attack action. With profit making gradually becomes the core of information security crime industrial chain, lots of bugs and attack tools being used commercially by criminals to get excessive profit, which makes information security threat range expand fast. After the explosion of “Prism”, network security construction in Malaysia has been promoted to national strategy position. The slogan “No network security, no national security” has been our consensus.

With national information security conscious increasing, the government and central enterprises have clearly shut the door for foreign anti-virus software with the purpose of independently controlling anti-virus software. As the core of anti-virus software business, LINKDOOD anti-virus software breaks monopoly phenomena of national market, which will bring national information security into a new era.

Detailed Design

Console Platform

Console Platform is deployed in enterprise’s private server and needs fixed IP address to ensure other endpoints to access through internet.

Console Platform is mainly used to communicate with endpoint, including receiving threat and log report from endpoints, distributing instruction and policy like scan threat, clear threat, update virus database and so on. Based on B/S mode, Console Platform allows administrator to remotely manage and view through browser, manage security condition of whole network, scan threat, clear threat, configure endpoint security policy and so on. Additionally, it provides update for endpoint’s client to update virus database and the Antivirus software. It also allows you to use quarantine network offline upgrade tool. You can download the upgrade data in a computer that has network, then import in Console Platform to update. Subsidiary console and all endpoints can also timely upgrade virus database and the Antivirus software.

Upgrade

LINKDOOD Antivirus provides several ways for users to upgrade software/virus database according to preset scene.

Internet Upgrade

In user’s environment, Console Platform is able to connect with internet. It sends a request to internet virus upgrade server each one-hour interval, if new version of the software and virus database found, they will automatically upgrade to the latest versions.

Quarantine Network Tool Upgrade

If Console Platform cannot connect with internet in user’s environment, but allows to use USB drive, quarantine network tool will preferentially upgrade in this circumstance. Quarantine network tool can update Trojan virus database of Console

Platform's server, system patch and program version, providing full protection for enterprises. Console Platform's System Management Center is available for you download quarantine network tool.

Script Upgrade

If user environment doesn't allow Console Platform to connect with internet and has to import data through CD, you can upgrade server virus database through executing script.

Management Function

LINKDOOD Antivirus software's Console Platform adopts B/S architecture, which helps administrator to have whole management in any device of internal network environment.

System Configuration

It is used to configure cascade function, which upper server can have central management of lower server, supporting multi-level cascade.

Security Condition

It shows overall security condition of intranet endpoints. By analyzing current infected endpoints, administrator can timely get to know the ratio between all endpoints and infected ones, which helps to avoid mass threats. It also displays threat trend, threat warning and virus infection status.

Threat Management

You can know virus scan and resolve information in current network through Console Platform. You can also sift information user needs through resolving status, threat level, virus type, virus file name and endpoint name. When finishing sifting, you can export the report.

Endpoint Management

You can view company/organization structure, console structure and all registered endpoints through Console Platform. By sifting condition, you can have operations for selected endpoint(s) such as scan threat, clear threat, distribute configuration, and delete endpoint and so on.

Audit Log

Audit Log provides multi-dimensional and multi-granularity log report and analysis report, completely managing information of the whole network.

Endpoint Audit Log

You can view operation log of all endpoints in server console platform. Through sifting condition like reason, operation type, time, operator's account, endpoint name to get information user needs, and the report can be exported when finishing sifting.

Admin Audit Log

You can view operation log of all administrators in in Console Platform. Through sifting condition like administrator level or type, operation type or target, time, administrator's account to get information user needs, and the report can be exported when finishing sifting.

Client

Active Defense

Through analyzing behavior and being driven by multi-engine, Active Defense can actively detect potential threats, smartly mark risk level and block them. Check sensitive boundary interface such as visit website, download software and copy file, which precisely intercept dangerous file and prevent risk from entering your computer.

Real-time Monitoring

Real-time Monitoring is able to monitor all processes running in your computer. LINKDOOD Antivirus can have real-time monitoring of your device. Once virus is found, it will automatically delete virus file or lock virus file to stop its running according to your settings. When you select "High" monitor level, LINKDOOD Antivirus will have the strictest protection of your computer. When you select "Standard" monitor level, LINKDOOD Antivirus will make sure the balance between security and performance. When you select "Low" monitor level, LINKDOOD Antivirus will protect key location and files to ensure system performance. When you select "Off" monitor, real time monitoring disables.

Virus Scan

By integrating various antivirus engines, LINKDOOD Antivirus V3 has strong virus scan & killing ability. Based on the needs of different users, LINKDOOD Antivirus provides three modes to scan virus, which you can select in the main interface.

Quick Scan

Quick Scan is to scan sensitive area like system folders in computer. Usually, when virus invades computer system, it will do some malicious modification in this area. Scanning this area helps to quickly detect and resolve most viruses, and the scanning speed is fast, only a few minutes.

Full Scan

Full Scan is to have a complete scanning of all files in computer. Some viruses not only damage system files but also do malicious behaviors to other parts. This mode will have a full scan of all files, thoroughly eliminating all virus files illegally invaded in the system.

Custom Scan

Custom Scan is to scan files in designated directory. You can choose one or several location according to your needs.

USB Protection

The system distributes file or installation software to designated client (user group), and provides software's running parameters and required running control method. This function can alleviate network manager's workload.

Threat Scan

USB Protection function o is able to automatically scan risky files in USB and send you notification about risk, which reduce the possibility of damaging your computer.

Quick-unplug

One clicks to quickly unplug your USB, protecting the data.

Quarantine & Recovery

Quarantine Zone

Risky file detected & cleared by active scan, real-time protection and USB protection will be put in quarantine zone. You can restore your trusted file in recovery zone or completely remove quarantined file.

Recovery Zone

Blocked and trusted action by Active Defense will be backup in Recovery Zone. You can manually restore them in this zone.

Trust Zone

Whitelist file(s) will put in Trust Zone, which file(s) here are deemed to be safe. LINKDOOD Antivirus will skip files in Trust Zone to speed up while scanning. Therefore, you should be careful when you want to add file to whitelist. If you add virus file to whitelist by mistake, it may lead to bad result.

Cloud

The main function of private cloud of LINKDOOD Antivirus V3 is to collect samples to check and give feedback about result to client.

Cloud Engine

The private cloud will store amount of operating system files and add safe files identified by cloud to whitelist. Meanwhile, cloud server will analyze suspicious files reported from users who participate in cloud scan plan. If a file is decided as threat, it will be added in blocked list. The hashes of these whitelist & blocked list files and property are stored in cloud, which facilitates client to scan effectively.

Characteristic-based Cloud Engine

Characteristic-based Cloud Engine scan faster and take smaller storage space. By learning from existing whitelist & blocked list samples, characteristic-based cloud engine finds the family characteristics among files. These characteristics replace hashes stored in cloud before, which greatly reduce storage cost of traditional hash

cloud. During scanning, it only extracts some segment’s information, and the speed is 3-5 times faster than calculating hash, which particularly works better for large files.

VDC Virus Idetification VDC

If client's local cache, local engine and cloud can't confirm detection result, client will upload unknown sample with a very slow speed of 20kb/ s. When it uploads successfully, private cloud's backend VDC will do detailed detection, such as sandbox behavior extraction, characteristics extraction. After offering result, VDC will update hash cloud and characteristic-based cloud engine.

Sample Collection

If VDC can't provide result for sample, LINKDOOD will collect sample manually and send to backend. Professional person will analyze these samples to confirm their property.